

Hard and Soft Safety Verifications

Jon Wetherholt, NASA Marshall Space Flight Center, Huntsville, Alabama, USA

Brenda Lindley Anderson Marshall Space Flight Center, Huntsville, Alabama, USA

Keywords: verification, launch vehicle, spacecraft

Abstract

The purpose of this paper is to examine the differences between and the effects of hard and soft safety verifications. Initially, the terminology should be defined and clarified. A hard safety verification is datum which demonstrates how a safety control is enacted. An example of this is relief valve testing. A soft safety verification is something which is usually described as “nice to have” but it is not necessary to prove safe operation. An example of a soft verification is the loss of the Solid Rocket Booster (SRB) casings from Shuttle flight, STS-4. When the main parachutes failed, the casings impacted the water and sank. In the nose cap of the SRBs, video cameras recorded the release of the parachutes to determine safe operation and to provide information for potential anomaly resolution. Generally, examination of the casings and nozzles contributed to understanding of the newly developed boosters and their operation. Safety verification of SRB operation was demonstrated by examination for erosion or wear of the casings and nozzle. Loss of the SRBs and associated data did not delay the launch of the next Shuttle flight.

Background

When producing a product there are customer requirements or federal regulations that must be verified before the product is allowed to be sold or used. Some verification is analytical, which requires modeling the product and the environment of operation. This requires empirical knowledge collected from previous similar products. Many verifications are levied on each individual item produced. For example, a car may be started before shipment or a launch vehicle may undergo a green run in which the engine is ignited and operated for an established period of time. Also, there are supplementary verifications for products which are not released for sale. In the case of the car, some vehicles are tested for impact effects, endurance and life. In the case of launch vehicles, an engine may be tested to limits well beyond its expected life or operation limits, while being thoroughly instrumented to collect supplementary data to further understanding of the operational limits of the engine. However, impact tests, not endured in commonplace car usage, do not consider every angle, velocity or vehicle which may be involved in an accident. Launch vehicle data from ground testing is limited to modeling, analysis, inspections. All launch vehicle testing is in a non-flight environment. Engine green runs do not endure the acceleration forces met in flight, or the vibration/pogo or change in nozzle pressure due to increase of altitude.

To obtain this data, production vehicles must be instrumented. Instrumentation and data recording may be relatively inexpensive, but data collection may present prohibitive costs. An automobile customer must bring the vehicle to a service department for information to be recorded. Launch vehicle data must be downlinked or recovered from a vehicle which generally lands in the ocean. Because data recovery can be expensive and sometimes the returns are difficult to determine, obtaining necessary funding to collect and process the data can be problematic.

Examples of Product Data Recording For Verification

This section will examine post-acceptance examples of data gathering, the results of which are used to improve a product or to provide verification that the service life of the product concurs with simulation modeling. Aircraft contain a Flight Data Recorder (FDR), commonly called a black box, which records parameters while the plane is in

flight. Most FDRs record such data as time, pressure, altitude, airspeed, vertical acceleration, magnetic heading, control-column position, rudder pedal position, control wheel position, horizontal stabilizer position and fuel flow. Such information often helps resolve the cause of an accident, such as mechanical failure or unforeseen environmental conditions like wind shear (Reference 1).

Automobiles have two methods of post-sale data recording, which can provide operating information similar to an FDR, and are often chosen to be installed by the purchaser in order to reduce insurance rates. A car's mileage and the time of day of operation can aid determining exposure to accidents. The automobile data recorders record such data as accelerations, quick stops and hard turns. The other automotive method of data collection is a mounted camera. Currently Progressive Insurance Company offers particular drivers a 30% reduction in rates if a camera is installed in the car. Operation and accident information is recorded by Event Data Recorders (EDR) on many newer cars, of whose existence the driver may not be aware (Reference 2). The EDR can provide such information as if the seat belt was buckled, the speed of the car, whether brakes were engaged, and steering angle. The National Highway Traffic Safety Administration (NHTSA) is currently considering a requirement for all new cars to have an EDR, in order to better understand accident conditions. Commercial trucking companies may use EDRs to determine if drivers are breaking laws.

Launch Vehicle Data Recording For Verification

Many previous launch vehicles had limited data recording because the data had to be down linked by costly telemetric means with limited bandwidth, or recovered from expended hardware. The weight margin for crewed flight vehicles was so restricted that equipment for recording ascent data was restricted. Before the advent of digital equipment, film was the only medium for obtaining visual data, which was generally heavy and complicated to retrieve. Staging on the Saturn V launch vehicle was recorded on film and ejected camera pods were parachuted to the ocean for recovery, which sometimes included several hours of search to locate. The film did, however, provide visual confirmation that staging had adequate clearance, and confirmation that other potential failure modes, which couldn't be simulated on the ground, had not occurred.



Staging video down linked from the Space X Falcon 9 demonstrated the significance of visual data by helping resolve a launch failure, the cause of which was inconclusive from telemetry data.

The advent of the Shuttle and the digital age provided opportunity to obtain detailed data and return it with the vehicle. The STS-1 strain gauges provided in-flight stress indications which indicated that the vehicle was near its load limit. This discovery led to changes in the ascent profile to reduce loading on the vehicle.

An important source of Shuttle operational data was the Operational Flight Instrumentation (OFI), which monitored physical sensors and logic signals that reported the status of various Orbiter functions (Reference 3). These sensor

readings and signals were telemetered via a 128 kilobit-per-second data stream to the ground, where engineers determined the real-time health of key Orbiter systems. This data was crucial to understanding the events during the Space Shuttle Columbia Accident (STS-107) for ascent, orbit, and re-entry.

Another data collection system on the Shuttle orbiter was the Modular Auxiliary Data System (MADS), which was a supplemental instrumentation system that gathered Orbiter data to be processed after the mission was completed. Inputs were typically physical sensor readings of temperatures, pressures, mechanical strains, accelerations, and vibrations. The MADS usually recorded only the first and last two hours of a mission.

Also, the Orbiter Experiment Instrumentation (EI) was an expanded suite of sensors for the MADS that was installed on Columbia for engineering development purposes. Engineering teams desired detailed flight data to validate their models of conditions the vehicle would experience in critical flight phases. The instrumentation remained on Columbia and continued through the life of the Orbiter to provide valuable flight data from ascent, de-orbit, and re-entry for ongoing flight analysis and vehicle engineering.

During STS 107 re-entry the MADS recorded the first abnormal condition while the Orbiter was still over the Pacific Ocean. Four sensors located inside and outside the wing leading edge spar near Reinforced Carbon-Carbon (RCC) panel 9-left provided information to reconstruct the events affecting the left wing of the Orbiter early in re-entry. These four sensors were: a strain gauge, resistance temperature detector on the RCC clevis between panel 9 and 10, a thermocouple within a Thermal Protection System tile, and a resistance temperature detector, located on the back side of the wing leading edge spar behind RCC panels 8 and 9.

Another suite of sensors provided data from the initial event, data from the strain gauges and temperature sensors in the left wing. The sensors can be seen in Figure 1, and the two graphs (Figures 2 and 3) show the output of those sensors. This information was critical in verifying the cause of the incident and resolving the initiating event which led to the wing damage.

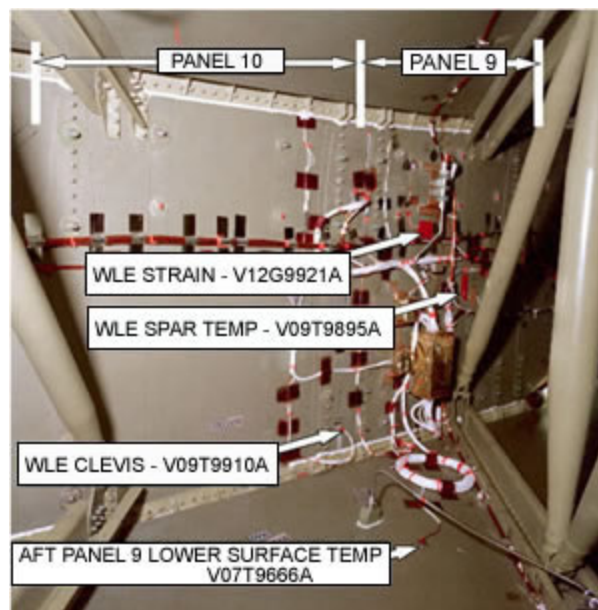


Figure 1 Strain Gauge Location on Columbia

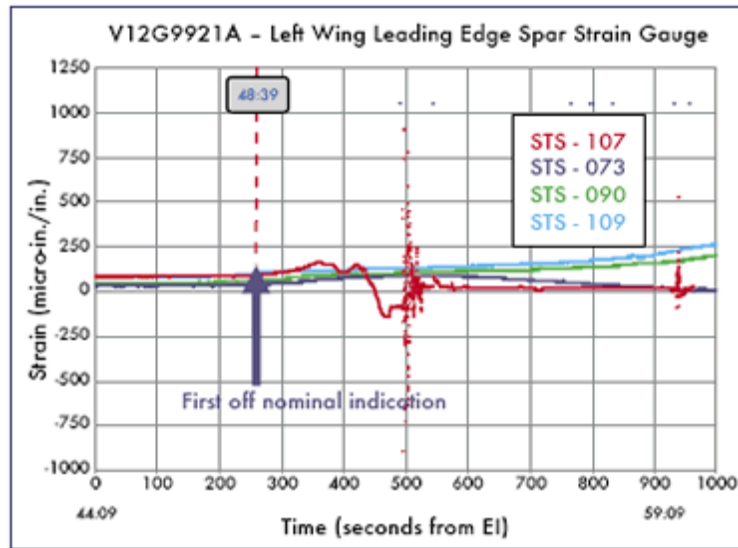


Figure 2 Columbia Left Wing Leading Edge Spar Strain Gage Data

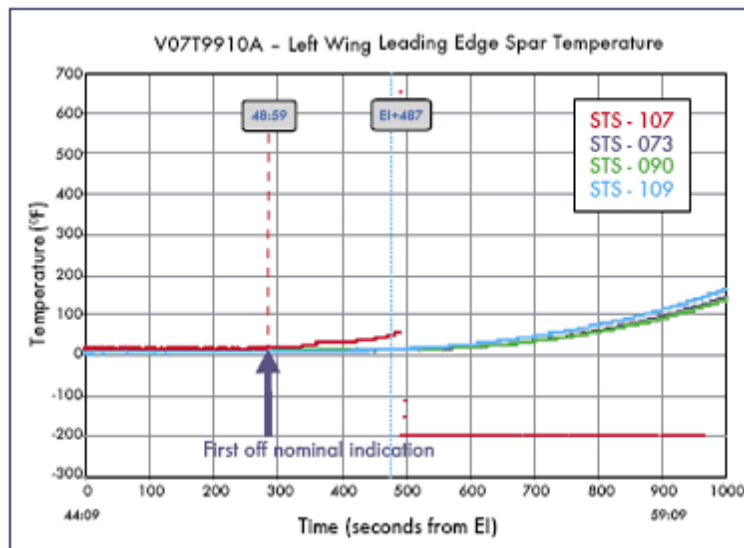


Figure 3 Left Wing Leading Edge Spar Temperature Data

Analysis

The commercial airplane industry comprehended early that data recording and analysis were vital to improving safety, which contributed to air travel being one of the safest modes of transportation. Shuttle post-flight acceptance data has prevented failures using data from both nominal flights as well as accident data. In order to duplicate this achievement in future applications, the data chosen for recording and processing must be significant data, and the time frame chosen for data examination should be near the end of the test phase when the product has the highest maturity before the operational phase. On many vehicles, NASA has two categories of instrumentation,

Development Flight Instrumentation (DFI) and Operational Flight Instrumentation (OFI). Generally, DFI is used only for developmental phase and may be removed or not installed on later vehicles in order to reduce weight or downlink requirements. The instrumentation and associated equipment creates hazards of its own, such as batteries and power systems which can create short circuits or fires, or antennae which can add stress on structure or generate debris. The OFI continues to be used provides flight data critical for determining trends in manufacturing/assembly, post-flight anomaly resolution or accident resolution.

Although the Shuttle returned a majority portion of the vehicle, this will likely not be the case in future launch vehicles. Therefore establishing what data is required to be recorded or down linked will be a challenging task. The engineers who develop launch systems wish to obtain necessary and sufficient data, minimally, to fully comprehend the system and verify their engineering assumptions and models used in manufacture and testing. Additional data beyond required information would only expand understanding, which will lead to better products in future vehicle developments. However, more and more, data collected is being restricted and limited. Managers, who have to provide money, mass and schedule for data recording systems and processing may see the need, but often can be an obstacle to obtaining even necessary data; expecting them to support supplementary data is improbable. Though imagery has proven particularly important in understanding both the Challenger and Columbia incidents, imagery recently has become viewed as not necessary, a soft requirement, and is being relegated to a lesser role, and in some cases, unnecessary. The first datum, which helped narrow the search for the culprit in the Challenger incident, was a film image of black smoke exiting a field joint on the left Solid Rocket Booster (SRB). In this time of tight budgets and enforced affordability above all other requirements, the focal role of imagery has been lost, considered a public relations device rather than valuable data.

Sensors and data recording are quickly becoming less expensive; therefore the cost to install a system to provide post-production information may be acceptable to some manufacturers, at least with earth-based items. The cost may shift to retrieval of data from customers, since they would have to bring the product to a central location, such as the dealer, with automobiles. Other products, such as boats or appliances, make data recovery arduous since they are serviced infrequently, and generally are not taken into a dealer. The data recovery from a space launch system is more complex still. For earth-bound uses, this may change in the future as appliances become more digitally connected and may be coupled to a home management system to monitor data indicating appliance health. If homes become more digitally connected, manufacturers could offer incentives to the customer to allow access to the data, perhaps as part of the warranty, similar to insurance companies lowering rates for automobiles with EDR. Then the manufacturer could easily monitor data to verify the parameters developed for life testing.

The challenge remains with launch vehicles. There is no easy way, at present, to bypass the difficulties of recovering certain data. Even making such systems digital doesn't solve the problems. Developing systems with longer range pickup can help eliminate some vehicle-based data collection, leaving the collection to a ground based system. This presents different obstacles. For imagery for example, the vehicle must be in line-of-sight for cameras to view. Also, the lens systems are limited in their ability to resolve some items as the vehicle travels further away from the camera system. Radar has proven useful as a substitute for cameras for observing the Shuttle. The parallel problem with sensor data is the ability to downlink over the horizon. Relay systems will still be required to collect the down linked data. Additionally, the more data that is down linked, the more the expense shifts to providing a system with enough bandwidth. Resolving this puzzle remains as the next breakthrough in space vehicle development.

Conclusions

Although it can be especially expensive to install sensors or cameras and record/recover or downlink data, the long term information provides better understanding of the product in actual usage. This understanding allows for verification of the product and improving the current product or the next generation. The greater the volume of data, the better the understanding of a product's behavior in operational usage, and the more accurate the estimation of

operational life for the average production item. Though minimum data recorded is most profitable to the company, maximum data recorded is more advantageous to the engineers who will be designing future products. Though some data item may be determined to be not necessary but only nice to have, these data items, nevertheless, increase product operation knowledge. Soft data requirements should not be dismissed out of hand simply because they are determined not necessary. Careful thought should be put into identifying data requirements, with an eye to verification rather than only expense. In the future, deliberation of final verification of product success should be concluded after actual usage application data is analyzed as a soft verification.

Appendix

The definition of verification is, according to Reference 4, establishment of the correctness of a theory, fact, etc.; evidence that provides proof of an assertion, theory, etc. or, 2. (Law) *law*; (formerly) a short affidavit at the end of a pleading stating the pleader's readiness to prove his assertions or confirmatory evidence.

References

Reference 1. <http://science.howstuffworks.com/transport/flight/modern/black-box5.htm>

Reference 2. http://en.wikipedia.org/wiki/Event_data_recorder

Reference 3. Columbia Accident Investigation Board Report Volume I August 2003

Reference 4 <http://www.thefreedictionary.com/verification>

Biography

Jon Wetherholt, NASA Marshall Space Flight Center, Huntsville, Alabama, 35812, USA Telephone (256) 544-4847, email – jon.c.wetherholt@nasa.gov

Mr. Wetherholt has more than 27 years of experience in system safety and product assurance. Mr. Wetherholt currently is the lead for SLS Vehicle Integration System Safety at the Marshall Space Flight Center in Huntsville, Alabama. He holds a BSME from the University of Akron and an MSME from the University of Toledo

Brenda Lindley Anderson, NASA Marshall Space Flight Center, Huntsville, Alabama, 35812, USA Telephone (256) 544-7071 brenda.l.anderson@nasa.gov

Ms Lindley Anderson has worked at MSFC for over 30 years with 23 years experience in space Shuttle main engine operation and technology. She worked system safety on several project studies before working system safety and vehicle integration on the Ares launch vehicle. Currently she is a safety team member for the Space Launch System program. She holds a BS in physics and a BS in mathematics, both from Jacksonville State University.